Commonwealth of Kentucky
Cabinet for Health and Family Services

Cabinet for Health and Family Services (CHFS) Information Technology (IT) Policy

065.016 Configuration Management

Version 2.2
December 15, 2017

Revision History

Date	Version	Description	Author
12/16/2011	1.0	Effective Date	CHFS IT Policies Team Charter
12/15/2017	2.2	Revision Date	CHFS OATS Policy Charter Team
12/15/2017	2.2	Review Date	CHFS OATS Policy Charter Team

Sign-Off

Sign-off Level	Date	Name	Signature
IT Executive, Office of the Secretary (or designee)	12/15/2017	ROBERT PUTT	
CHFS Chief Security Officer (or designee)	12/15/2017	DENNIS E. LEBER	

Table of Contents

065.016 Configuration Management

Category: 065.000 Application Development

1 Policy Overview

1.1 Purpose

The Cabinet for Health and Family Services (CHFS) Office of Administrative and Technology Services (OATS) must establish an acceptable level of security controls to be implemented through a configuration management policy. This document establishes the agency's Application Configuration Management Policy to manage risks and provide guidelines for security best practices regarding configuration management.

1.2 Scope

The scope of this policy applies to all internal CHFS employees, consultants, temporary personnel, third party providers under contract with a CHFS agency, and other entities that interact with CHFS information related resources. This policy covers the applicable computer hardware, software, application, configuration, business data, and data communication systems. External vendors providing information security or technology services may work with the CHFS agency(s) to request exceptions to this policy.

This policy applies to all systems and/or applications implemented subsequent to the 2017 policy review/revision date. Systems and/or applications implemented prior to the 2017 policy review/revision will be considered for compliance with this policy based upon consideration of priority, resources, and funding availability.

1.3 Management Commitment

This policy has been approved by OATS Division Directors, CHFS Chief Technical Officials, and Office of the Secretary IT Executive. Senior Management supports the objective put into place by this policy. Violations may result in disciplinary action, which may include suspension, restriction of access, or more severe penalties up to and including termination of employment. Where illegal activities or theft of CHFS property (physical or intellectual) are suspected, CHFS may report such activities to the appropriate authorities.

1.4 Coordination among Organizational Entities

OATS coordinates with other organizations or agencies within CHFS with access to applications or systems. All organizational entities that interact with CHFS systems, within or contracted by OATS, are subject to follow requirements outlined within this policy. External vendors, or other defined groups/organizations, providing information security or technology services may work with the CHFS agency(s) when seeking an exception to this policy.

1.5 Compliance

As the official guidance domain for this policy, CHFS agencies abide by the security and privacy requirements established in state laws and regulations as well as federal guidelines outlined in the National Institute of Standards and Technology (NIST). Applicable agencies additionally follow security and privacy frameworks outlined within the Centers for Medicare and Medicaid Services (CMS), the Internal Revenue Services (IRS), and the Social Security Administration (SSA).

2 Roles and Responsibilities

2.1 Chief Information Security Officer (CISO)

This positon is responsible for the assessment, planning, and implementation of all security standards, practices, and commitments required. This designated position is responsible to adhere to this policy.

2.2 Security/Privacy Lead

Individual(s) designated by the division leadership to coordinate privacy and/or security issues and incidents with all appropriate personnel. This individual(s) is responsible for providing privacy and security guidance for protection of Personally Identifiable Information (PII), Electronic Personal Health Information (ePHI), Federal Tax Information (FTI) and other sensitive information to all CHFS staff and contractor personnel. This role is responsible for the adherence of this policy along with the CHFS OATS Information Security (IS) Team.

2.3 Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer

An attorney within CHFS Office of Legal Services (OLS) fills the Health Insurance Portability and Accountability Act (HIPAA) Privacy Officer position. This position is responsible for conducting HIPAA mandated risk analysis on information provided by the CISO or CHFS OATS IS Team. The HIPAA Privacy Officer will coordinate with the Information Security Agency Representative, the CISO or CHFS OATS IS Team, and other CHFS agencies to ensure compliance with HIPAA notification requirements in the event of a breach. This position will be responsible for reporting identified HIPAA breaches to Health and Human Services (HHS) Office of Civil Rights (OCR) and keeping records of risk analyses, breach reports, and notification in accordance with HIPAA rules and regulations.

2.4 CHFS Staff and Contractor Employees

All CHFS staff, contract employees, and other applicable vendor/contract staff must adhere to this policy. All personnel must comply referenced documents that pertain to the agency's applications, application servers, appliances, operating systems, web servers, network components, and database (server or components) that reside on CHFS/OATS information system(s).

2.5 System Data Owner and System Data Administrators

It is the responsibility of these management/lead positons, to work with the application's development team to document components that are not included in the base server build and ensure backups are conducted in line with business needs. This individual(s) responsibilities are to work with Enterprise, agency, and application technical and business staff to provide full recovery of all the application functionality and meet federal and state regulations for disaster recovery situations.

3 Policy Requirements

3.1 Baseline Configuration

CHFS agencies follow the Commonwealth Office of Technology (COT) OIS-053 Windows and ESX Baseline Configuration Documentation Annual Review Procedure. This finalized process establishes the baseline security configuration for all windows systems supported by the COT windows Server Support Team. CHFS follows Enterprise OIS-051 Security Configuration Documentation Annual Review Procedure by reviewing baselines and updates for desktop, laptop and printer components annually and during critical system patches, emergency patches, and/or major system updates, as required.

COT is responsible for retaining older versions of baseline configurations for CHFS agencies servers, laptops, desktops, printers, network switches, and firewall components. The CHFS agencies will retain configurations, current and past versions, for software components.

3.2 Configuration Change Control

CHFS agencies follow the CHFS 010.103- Change Control Policy and CHFS 065.014- CHFS SDLC and New Application Development Policy regarding change control guidelines. The CHFS agencies and/or the enterprise will retain records of configuration-controlled changes to the Information System for a minimum of three (3) years.

3.3 Access Restrictions for Change

To ensure software application updates are reviewed and implemented in a rational and predictable manner, the following policies/procedure must be followed by CHFS agencies to document significant changes to software, hardware, communication links, and operational procedures:

- Enterprise Policy CIO-101 Enterprise Release Management Policy.
- Enterprise Procedure: COT-067- Enterprise Security Standard Process and Procedures Manual (ESSPPM) Section 5.7.6- Hardware Changes/Configuration Management
- Enterprise Procedure: COT-009 Change Management

3.4 Configuration Settings

CHFS agencies will follow COT security configuration guidelines, which include mandatory baseline configuration settings for information systems. Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following CHFS 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Controls Policy, or the formal COT Security Exemption Request, COT-F085 form process.

3.5 Least Functionality

CHFS agencies are required to design systems based on the principle to provide only essential capabilities. COT prohibits and disables the use of high-risk system services, ports, network protocols, and capabilities across network boundaries that are not explicitly required for system or application functionality. COT supports the entire Commonwealth infrastructure for the agencies.

COT performs monthly vulnerability scans of networks, servers and databases to identify unnecessary functions, ports, protocols and/or services. Based on the scanning results, COT coordinates with necessary agency personnel to remediate/disable unnecessary functions, ports, protocols, and/or services identified.

3.6 Information System Component Inventory

COT shall utilize the Procurement, Payables, and Asset Tracking System (PPATS) for tracking IT hardware assets through their lifecycle from procurement to disposal. Along with the PPATS system, COT Asset Management Division maintains an up-to-date inventory of software under its control for quality assurance.

3.7 Configuration Management Plan

OATS IS Team recommends each agency to develop, document, and implement a configuration management plan for the information system. This plan should include, but is not limited to:

- Addressing roles, responsibilities, configuration management processes, and procedures;
- Establishing a process for identifying configuration items throughout the systems

development lifecycle (SDLC) and managing the configuration of items;

- Defining configuration items for information systems and place the configuration items under configuration management;
- Protecting the configuration management plan from unauthorized disclosure and modification;

National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems- Appendix D can be referenced and used as a guide/sample for agencies when creating a configuration management plan.

3.8 Software Usage Restrictions and User Installed Software

COT Division of Asset Management is responsible for periodically reviewing compliance of software licenses and copyright policies. Additionally, each COT department's management is responsible for ensuring that the necessary documentation is available to provide proof of proper software acquisition.

COT-067: ESSPPM, Section 3- Logical Security Processes and Procedures ensures standardized configurations for hardware and software. For security reasons, installation of unauthorized applications is not permitted on the network. Any unauthorized applications will be removed and the use may be subject to disciplinary actions.

Any exceptions from these mandatory configurations must go through the formal CHFS approval process by following the Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027, or the formal COT exception process following Security Exemption Request, COT-F085.

4 Policy Definitions

- **Agency:** for the purpose of this document, agency or agencies refers to any department under CHFS.
- **Baseline Configuration:** per the National Institute of Standards and Technology, it is a set of specifications for a system, or CI within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.
- **Confidential Data:** as defined by COT standards, is data of which the Commonwealth has a legal obligation to not disclose. This data requires the highest levels of restrictions, because of the risk or impact that will result from disclosure, modification, breach, or destruction. Examples include, but are not limited to: data not releasable under the Kentucky State law, Protected Health Information, Federal Tax Information, and Social Security and Credit Card Numbers.

- **Sensitive Data:** as defined by COT standards, is data that is not legally protected, but should not be considered public information and only be disclosed under limited circumstances. Only authorized users should be granted access to sensitive data. Examples include, but are not limited to: information identifiable to an individual (i.e. date of birth, driver's license numbers, employee ID numbers, license plate numbers, and compensation information) as well as the Commonwealth proprietary information (i.e. intellectual property, financial data, and more.)

5 Policy Maintenance Responsibility

The CHFS OATS IS Team is responsible for the maintenance of this policy.

6 Policy Exceptions

Any exceptions to this policy must follow the guidance established in CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy.

7 Policy Review Cycle

This policy is reviewed at least once annually, and revised on an as needed basis.

8 Policy References

- Centers for Medicare and Medicaid Services (CMS) MARS-E 2.0
- CHFS OATS Policy: 010.103- Change Control Policy
- CHFS OATS Policy: 065.014 CHFS SDLC and New Application Development Policy
- CHFS OATS Policy: 070.203- Security Exceptions and Exemptions to CHFS OATS Policies and Security Control Policy
- CHFS Procurement, Payables, and Assets Tracking System
- Enterprise IT Policy: CIO-101- Enterprise Release Management Policy
- Enterprise IT Procedure: COT-067: Enterprise Security Standard Process and Procedures Manual (ESSPPM)
- Enterprise IT Procedure: OIS-051- Security Configuration Documentation Annual Review Procedure for Printers, Desktops, and Laptops Procedure
- Enterprise IT Procedure: OIS-053- Windows and ESX Baseline Configuration Documentation Annual Review Procedure
- Enterprise Security Exemption Request, COT-F085
- Enterprise Kentucky Information Technology Standards (KITS) Exception Request Form, COT-027
- Internal Revenue Services (IRS) Publication 1075

- Kentucky Information Technology Standards (KITS): 4080 Data Classification Standard
- National Institute of Standards and Technology (NIST) Special Publication 800-12 Revision 1, Introduction to Information Security (Draft)
- National Institute of Standards and Technology (NIST) Special Publication 800-18 Revision 1, Guide for Developing Security Plans for Federal Information Systems
- National Institute of Standards and Technology (NIST) Special Publication 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations
- National Institute of Standards and Technology (NIST) Special Publication 800-128 Revision 1, Guide for Security-Focused Configuration Management of Information Systems
- Social Security Administration (SSA) Security Information